

ResearchOnline@JCU

This is the **Accepted Version** of a paper published in the
Journal of Cryptology

Ghodosi, Hossein (2013) *Analysis of an unconditionally
secure distributed oblivious transfer*. Journal of Cryptology,
26 (1). pp. 75-79.

<http://dx.doi.org/10.1007/s00145-011-9113-2>

Analysis of An Unconditionally Secure Distributed Oblivious Transfer

Hossein Ghodosi

Department of Information Technology, School of Business
James Cook University, Townsville, Qld 4811, Australia

Abstract. In the Journal of Cryptology (vol 20, no. 3), Blundo, D’Arco, De Santis and Stinson proposed a general model for unconditionally secure distributed oblivious transfer (DOT), where a sender has n secrets and a receiver is interested to one of them.

We show that their t -private weak one-round (k, m) -DOT $\binom{n}{1}$ protocol cannot prevent a receiver who attempts to obtain more than one secret. We present a modification to Blundo et al.’s protocol that fixes this problem.

Keywords: Oblivious transfer, Secret sharing, Distributed cryptography.

1 Introduction

Oblivious transfer (OT) protocols [6, 2] allow two interacting parties, Alice as a sender and Bob as a receiver, to exchange a secret message in an oblivious way. Execution of these OT protocols, however, requires the availability of the unique sender. Naor and Pinkas [5] introduced the concept of 1-out-of-2 distributed oblivious transfer (DOT), where Alice is replaced with m servers. In [1], Blundo, D’Arco, De Santis, and Stinson generalize Naor and Pinkas’s 1-out-of-2 DOT protocol to a 1-out-of- n DOT protocol.

A fundamental requirement of every OT protocol is to guarantee that the receiver cannot learn anything about the secrets that he is not supposed to learn. We show that Blundo et al.’s t -private weak one-round (k, m) -DOT $\binom{n}{1}$ protocol cannot prevent a receiver who attempts to obtain more than one secret. We present a modification to their protocol that fixes this problem.

2 A Brief Review of Blundo et al.’s DOT Protocols

In a 1-out-of- n DOT protocol, the sender has n secrets, w_0, \dots, w_{n-1} , and the receiver is interested in one of them, say w_i , where $i \in \{0, \dots, n-1\}$. The protocol has two phases: (i) the set-up phase and (ii) the oblivious transfer phase. In the set-up phase of the protocol, the sender provides some information to each server. Then, in the oblivious transfer phase, the receiver needs to communicate with at least k servers in order to obtain the desired secret, where $k < m$. In [1], such a protocol is called a (k, m) -DOT- $\binom{n}{1}$.

Blundo et al. have claimed that a (k, m) -DOT- $\binom{n}{1}$ protocol must satisfy the following properties:

1. **Correctness.** Using the information acquired during the protocol execution (that involves interaction with k out of m servers), the receiver can compute the chosen secret w_i .
2. **Receiver’s privacy.** No coalition of less than k servers can determine which secret the receiver has recovered.

3. Sender's privacy with respect to $k - 1$ servers and the receiver. A coalition of the receiver with $k - 1$ dishonest servers does not learn any information about the secrets.
4. Sender's privacy with respect to a "greedy" receiver. Given the transcript of the interaction with k servers, the receiver should gain information about at most a single secret, and no information about the others. This property should be satisfied even if the receiver colludes with $k - 1$ dishonest servers once he has computed a secret.

In [1], Blundo et al. proposed a one-round protocol based on polynomial interpolation that satisfies the first three properties. They have stated that in DOT protocols with only one round of interaction it is impossible to achieve the fourth property. However, they have proposed a t -private one-round (k, m) -DOT- $\binom{n}{1}$ for achieving sender's privacy with respect to a coalition among the receiver and a subset of t servers, where $t < k - 1$. This protocol is shown in Figure 1.

A sub-protocol for t -private weak one-round (k, m) -DOT- $\binom{n}{1}$ (see [1])

Let $w_0, w_1, \dots, w_{n-1} \in F_P$ be the sender's secrets, and let $i \in \{0, \dots, n-1\}$ be the receiver's choice.

Set-up Phase

- Let d_x, d_y and d_z be integers such that $d_x + d_z d_y(n-1) = k - 1$. The sender generates $r_0, r_1, \dots, r_{n-1} \in_R F_P$, and sets up an n -variate polynomial with values in F_P :

$$Q(x, y_1, \dots, y_{n-1}) = \sum_{j=0}^{d_x} \sum_{\ell_1=0}^{d_y} \dots \sum_{\ell_{n-1}=0}^{d_y} a_{j, \ell_1, \dots, \ell_{n-1}} x^j y_1^{\ell_1} \dots y_{n-1}^{\ell_{n-1}},$$

where $a_{0, \dots, 0} = r_0 w_0$, for $i = 1, \dots, n-1$, $\sum_{\ell_i=0}^{d_y} a_{0, \dots, \ell_i, \dots, 0} = r_i w_i$, and all other coefficients are chosen uniformly at random. It follows that $Q(0, 0, \dots, 0) = r_0 w_0$, $Q(0, 1, 0, \dots, 0) = r_1 w_1, \dots$, $Q(0, 0, \dots, 0, 1) = r_{n-1} w_{n-1}$.

- Then the sender constructs Shamir (k, m) -threshold scheme [7] for the secret r_ℓ , where $\ell = 0, \dots, n-1$. Let r_ℓ^j , for $j = 1, \dots, m$, be the corresponding shares. For $j = 1, \dots, m$, the sender sends the $(n-1)$ -variate polynomial $Q(j, y_1, \dots, y_{n-1})$ and the shares r_0^j, \dots, r_{n-1}^j to the server S_j .

Oblivious Transfer Phase

- The receiver chooses $n-1$ random polynomials $Z_1(x), \dots, Z_{n-1}(x)$ of degree d_z such that $(Z_1(0), \dots, Z_{n-1}(0))$ is an $(n-1)$ -tuple of zeros if $i = 0$ or an $(n-1)$ -tuple of zeros and a single one at the position i , if $i \in \{1, \dots, n-1\}$.
- The receiver chooses a subset $X \subseteq \{0, \dots, n-1\}$ of k indices, and for every $j \in X$, the values $Z_1(j), \dots, Z_{n-1}(j)$ are sent to the server S_j . He then receives the values $V(j) = Q(j, Z_1(j), \dots, Z_{n-1}(j))$, and all the shares r_0^j, \dots, r_{n-1}^j .
- After receiving the k values $V(j)$, for $j \in X$, the receiver interpolates a univariate polynomial $V(x) = Q(x, Z_1(x), \dots, Z_{n-1}(x))$ of degree $k-1$, and computes $V(0)/r_i$ where r_i is constructed through the shares r_i^j .

Fig. 1. A sub-protocol for t -private weak one-round (k, m) -DOT- $\binom{n}{1}$

3 Analysis of Blundo et al.'s DOT Protocol

In the sub-protocol of a t -private weak one-round (k, m) -DOT- $\binom{n}{1}$ protocol, the receiver is required to choose $n-1$ random polynomials, $Z_1(x), \dots, Z_{n-1}(x)$, of degree d_z such that $Z_1(0) = Z_2(0) = \dots = Z_{n-1}(0) = 0$ if $i = 0$ or $Z_i(0) = 1$ for a single value $i \in \{1, \dots, n-1\}$ and $Z_j(0) = 0$

for all values $j \neq i$. In their paper, Blundo et al. state that if the receiver contacts k servers, he obtains one and only one secret, w_i , of his choice. This is because if the receiver chooses polynomials $Z_1(x), \dots, Z_{n-1}(x)$ of degree d_z , the polynomial $V(x) = Q(x, Z_1(x), \dots, Z_{n-1}(x))$ interpolated by the receiver will be of degree $k-1$, and therefore can be reconstructed from the information obtained from k servers.

We observe that, if the chosen polynomials $Z_1(x), \dots, Z_{n-1}(x)$ are of degree less than d_z , then polynomial $V(x)$ will be of degree less than $k-1$, and thus can be interpolated using fewer than k points. For example, if $d_z = 0$, the resulting polynomial $V(x)$ will be of degree d_x , and therefore can be interpolated with information obtained from $d_x + 1$ servers. This is because the response of each server provides information about one point associated with the $V(x)$ polynomial. The following example illustrates a possible attack by the receiver on the sender's privacy, in the t -private weak one-round (k, m) -DOT- $\binom{n}{1}$ protocol.

Example 1. Assume that the sender has four secret values, w_0, w_1, w_2, w_3 , and she chooses the integers $d_x = d_y = d_z = 2$. Therefore, $d_x + d_z d_y (n-1) = k-1 = 18$, thus the receiver is allowed to contact 19 servers in order to learn one and only one of the secret values w_0, w_1, w_2, w_3 . However, if the receiver chooses polynomials $Z_1(x), Z_2(x), Z_3(x)$ of degree 0, the interpolated polynomial $V(x)$ will be of degree $d_x = 2$, which can be reconstructed from the responses of only three servers. As a result, the receiver learns all secrets.

Remark – Generating polynomials of exact degree $d_z = d_x$, although prevents the receiver from learning more than one secret, breaches the receiver's privacy (see below).

Theorem 1. [4, 3] *Given a Shamir (k, n) threshold scheme, if the degree of the associated polynomial $f(x) = S + a_1x + \dots + a_{k-1}x^{k-1}$ is known to be $k-1$ (i.e. $a_{k-1} \neq 0$), then the scheme is not perfect.*

In the light of Theorem 1, if Blundo et al.'s protocol has a mechanism that forces the degree of the polynomials chosen by the receiver be of degree d_z , a coalition of d_z servers may learn the choice of the receiver. The following example demonstrates this threat.

Example 2. Let servers S_1, \dots, S_{d_z} collaborate in order to possibly learn the receiver's choice. They will construct polynomials $Z'_j(x)$ (for $j = 1, \dots, n-1$) of degree at most $d_z - 1$. For each polynomial, if $Z'_j(0) = 1$, they learn that w_j is not the chosen secret (because the d_z -degree polynomial $Z_j(x)$ chosen by the receiver must satisfy $Z_j(0) = 0$). However, if one of the interpolated polynomials $Z'_\ell(x)$, for $\ell \in \{1, \dots, n-1\}$, satisfies $Z'_\ell(0) = 0$, the collaborating servers learn that w_ℓ is the choice of the receiver. This breaches the privacy of the receiver, since it is claimed (see page 355 of [1]) that the protocol satisfies the property of receiver's privacy against a coalition of d_z servers.

Note that for all indices $j \in \{1, \dots, n-1\}$, if $Z'_j(0) \notin \{0, 1\}$, the collaborating servers learn nothing about the choice of the receiver regarding w_j .

We acknowledge that Blundo et al.'s protocol states the randomness of $Z_j(x)$ polynomials, and thus privacy of the receiver is guaranteed.

4 A Modified t -private Weak One-round (m, k) -DOT- $\binom{n}{1}$ Protocol

Our analysis show that in the t -private weak one-round (k, m) -DOT- $\binom{n}{1}$ protocol, achieving privacy of the receiver implies the polynomials $Z_j(x)$ chosen by the receiver be of degree at most d_z (not

exactly of degree d_z). In the meantime, the receiver must not be able to utilize the lower degree polynomials $Z_j(x)$ for learning more secrets. Both requirements can be satisfied if $Z_j(x)$ polynomials are chosen randomly, such that neither the servers nor the receiver know their exact degrees. A possible solution is as follows:

1. In the set-up phase, in addition to existing steps, the sender generates $n-1$ random polynomials $u_j(x)$ of degree at most d_z , subject to $u_j(0) = 0$ (for all $j = 1, \dots, n-1$), and gives each server, S_j , a vector $U_j = (u_1(j), \dots, u_{n-1}(j))$.
2. In the oblivious transfer phase, each contacted server, S_j , instead of responding

$$V(j) = Q(j, Z_1(j), \dots, Z_{n-1}(j)),$$

responds

$$V(j) = Q[j, (Z_1(j) + u_1(j)), \dots, (Z_{n-1}(j) + u_{n-1}(j))].$$

This minor modification, which adds a zero polynomial to every $Z_j(x)$ polynomial chosen by the receiver, guarantees the truly randomness required by Blundo et al.'s protocol. It maintains the privacy of the receiver, and prevents the above-mentioned attack by the receiver.

Acknowledgments

The author gratefully acknowledge the insightful comments of the anonymous referees that leads to the modification of the protocol.

References

1. Blundo, C., D'Arco, P., Santis, A.D., Stinson, D.: On Unconditionally Secure Distributed Oblivious Transfer. *Journal of Cryptology* 20(3), 323–373 (2007)
2. Even, S., Goldreich, O., Lempel, A.: A Randomized Protocol for Signing Contracts. *Communications of the ACM* 28(6), 634–647 (1985)
3. Ghodosi, H.: On insecurity of Naor-Pinkas' distributed oblivious transfer. *Information Processing Letters* 104(5), 179–182 (2007)
4. Ghodosi, H., Pieprzyk, J., Safavi-Naini, R.: Remarks on the Multiple Assignment Secret Sharing Scheme. In: Han, Y., Okamoto, T., Qing, S. (eds.) *Proceedings of ICICS'97 –International Conference on Information and Communications Security*, Beijing, P. R. China, *Lecture Notes in Computer Science*, vol. 1334, pp. 72–80. Springer-Verlag (Berlin) (1997)
5. Naor, M., Pinkas, B.: Distributed Oblivious Transfer. In: Okamoto, T. (ed.) *Advances in Cryptology - Proceedings of ASIACRYPT 2000*, *Lecture Notes in Computer Science*, vol. 1976, pp. 205–219. Springer-Verlag (2000)
6. Rabin, M.: How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, USA (1981)
7. Shamir, A.: How to Share a Secret. *Communications of the ACM* 22(11), 612–613 (Nov 1979)